URI HIPAA SECURITY POLICY – IMPLEMENTATION SPECIFICATION #7E

Title:	**APPLICATIONS AND DATA CRITICALITY ANALYSIS**	**Purpose & Background**	**See Memo Entitled "HIPAA at URI: Introduction to HIPAA and an Overview of HIPAA Implementation at URI" available online at the URI HIPAA website**
Originator (Responsible Department/ Unit):	**URI HIPAA Compliance Oversight Committee**	**Effective Date:**	**05/22/2018**
Applies to:	**All URI Departments and Units Designated as HIPAA "Covered Components" and "Business Associate Components"**	**Revised Date(s):**	

Purpose:

This implementation specification reflects URI's commitment to conduct an annual analysis of the criticality of its healthcare computing systems.

Specification:

URI Covered Entities must have a formal process for defining and identifying the criticality of its healthcare computing systems and the data contained within them. The prioritization of URI information systems must be based on an analysis of the impact to URI services, processes, and business objectives if disasters or emergencies cause specific information systems to be unavailable for particular periods of time. The criticality analysis must be conducted with significant involvement from the administrators, users, and owners of URI information systems and business processes. The criticality analysis must be conducted at least annually.

Procedure:

1. URI Covered Entities must have a formal, documented process for defining and identifying the criticality of its information systems and the data contained within them. At a minimum, the process must include:

    - Creating an inventory of interdependent systems and their dependencies.
    - Documenting the criticality of URI's information systems.
    - Identifying and documenting the impact to URI Covered Entity services, if specific URI information systems are unavailable for different periods of time (e.g. 1 hour, 1 day).
    - Identifying the maximum time periods that healthcare computing systems can be unavailable.
    - Prioritizing healthcare computing system components according to their criticality to the Covered Entity's ability to function at normal levels

2. The criticality analysis must be conducted at least annually. The criticality analysis report must be securely maintained.

HIPAA REGULATORY REFERENCE: 45 CFR 164.308(a)(7)(ii)(E)
HIPAA SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE: *"Assess the relative criticality of specific applications and data in support of other contingency plan components"*